

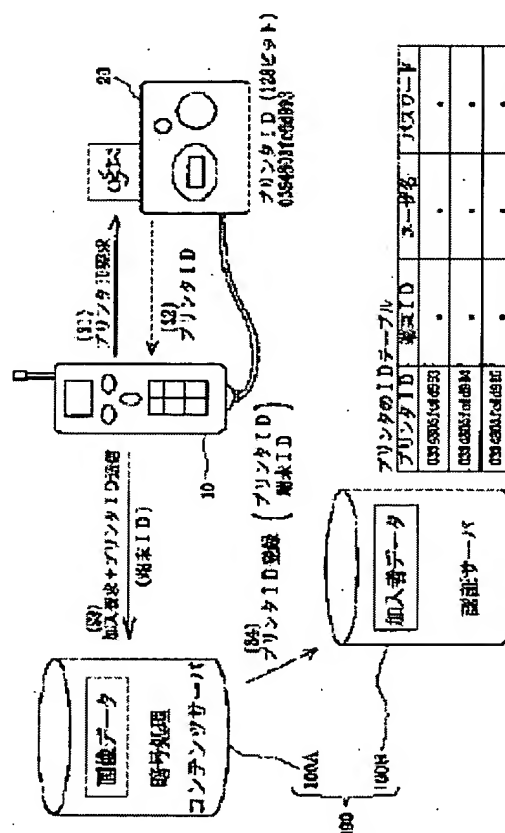
METHOD FOR REGISTERING USER TO CONTENTS SERVER

Patent number: JP2002305514
Publication date: 2002-10-18
Inventor: UEHATA MASAKAZU; HOSOI YUJI; EBISAWA RYOJI
Applicant: SEIKO INSTR INC
Classification:
 - international: **H04L9/08; H04Q7/38; H04L9/08; H04Q7/38; (IPC1-7): H04L9/08; G06F17/60; H04Q7/38**
 - european:
Application number: JP20010108508 20010406
Priority number(s): JP20010108508 20010406

Report a data error here

Abstract of JP2002305514

PROBLEM TO BE SOLVED: To provide a method for registering a user to a contents server, that highly keeps the security with respect to distribution of contents data with a simple method and distributes the contents data while keeping high security of a peripheral unit connected to a terminal.
SOLUTION: This user registration method, for registering a device ID of a peripheral device 20, which is connected to a terminal and is provided with the device ID being an encryption key and a decoding means, through the terminal connected to the contents server via a network, comprises a step of acquiring the device ID of the peripheral device 20 together with a user identification ID from the user making a subscription request by using the terminal 10 connected to the contents server via the network and connected to the peripheral device 20, a step of deciding a user ID with respect to a combination of the user identification ID and the device ID, and a step of selecting the user ID with respect to the combination of the user identification ID and the device ID for an access ID and registering the user by using the device ID for the encryption key for contents distribution.



Data supplied from the esp@cenet database - Worldwide

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-305514

(P2002-305514A)

(43)公開日 平成14年10月18日(2002. 10. 18)

(51)IntCl.⁷

識別記号

F I

テマコード*(参考)

H 0 4 L 9/08

G 0 6 F 17/60

1 4 2

5 J 1 0 4

G 0 6 F 17/60

1 4 2

3 0 2 E

5 K 0 6 7

3 0 2

5 1 2

5 1 2

H 0 4 L 9/00

6 0 1 Z

H 0 4 Q 7/38

H 0 4 B 7/26

1 0 9 S

審査請求 未請求 請求項の数 8 O L (全 8 頁) 最終頁に続く

(21)出願番号 特願2001-108508(P2001-108508)

(71)出願人 000002325

(22)出願日 平成13年4月6日(2001. 4. 6)

セイコーインスツルメンツ株式会社
千葉県千葉市美浜区中瀬1丁目8番地(72)発明者 上畑 正和
千葉県千葉市美浜区中瀬1丁目8番地 セイコーインスツルメンツ株式会社内(72)発明者 細井 雄次
千葉県千葉市美浜区中瀬1丁目8番地 セイコーインスツルメンツ株式会社内(74)代理人 100096378
弁理士 坂上 正明

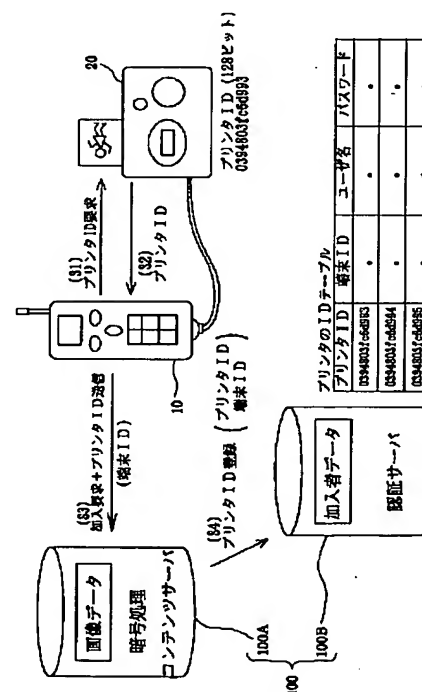
最終頁に続く

(54)【発明の名称】 コンテンツサーバへのユーザ登録方法

(57)【要約】

【課題】 コンテンツデータの配信に関してのセキュリティを簡便な手法で高度に保持して配信するコンテンツサーバへ、端末装置に接続される周辺機器からの高セキュリティを保持してユーザ登録する方法を提供する。

【解決手段】 ネットワークを介してコンテンツサーバ100へ接続する端末装置を介して、当該端末装置に接続され且つ暗号鍵となる機器ID及び復号化手段を具備する周辺機器の機器IDを前記コンテンツサーバへ登録するユーザ登録方法であって、前記周辺機器20を接続した端末装置10から前記ネットワークを介して接続して加入要求をしたユーザから、前記ユーザ識別IDと共に前記周辺機器20の機器IDを取得する工程と、前記ユーザ識別ID及び前記機器IDの組合わせに対してユーザIDを決定する工程と、前記通信端末装置及び前記周辺機器の組合わせに対して前記ユーザIDを接続IDとすると共に前記機器IDをコンテンツ配信の暗号鍵としてユーザ登録する工程とを具備する。



【特許請求の範囲】

【請求項 1】 ネットワークを介してコンテンツサーバへ接続する端末装置を介して、当該端末装置に接続され且つ暗号鍵となる機器 ID 及び復号化手段を具備する周辺機器の機器 ID を前記コンテンツサーバへ登録するユーザ登録方法であって、

前記周辺機器を接続した端末装置から前記ネットワークを介して接続して加入要求をしたユーザから、前記ユーザ識別 ID と共に前記周辺機器の機器 ID を取得する工程と、

前記ユーザ識別 ID 及び前記機器 ID の組合わせに対してユーザ ID を決定する工程と、

前記通信端末装置及び前記周辺機器の組合わせに対して前記ユーザ ID を接続 ID とすると共に前記機器 ID をコンテンツ配信の暗号鍵としてユーザ登録する工程とを具備することを特徴とするユーザ登録方法。

【請求項 2】 前記端末装置がパソコンであり、USB ポートに接続された暗号解読装置であることを特徴とする請求項 1 に記載のユーザ登録方法。

【請求項 3】 前記端末装置が通信端末装置であり、前記ユーザ識別 ID を当該通信端末固有の端末 ID とし、前記接続 ID を、前記ユーザ ID 及び前記端末 ID を接続 ID とすることを特徴とする請求項 1 に記載のユーザ登録方法。

【請求項 4】 前記ユーザ ID を決定する際に接続するためのパスワードを決定することを特徴とする請求項 1 ～ 3 の何れかに記載のユーザ登録方法。

【請求項 5】 前記機器 ID の取得は、前記周辺機器から機器 ID を受信することにより行うことを特徴とする請求項 1 ～ 4 の何れかに記載のユーザ登録方法。

【請求項 6】 前記機器 ID が所定グループに依存するグループ ID 部と機器固有 ID 部とからなり、前記グループ ID 部は前記所定グループ毎に予め登録されており、当該機器 ID の取得は、前記周辺機器から前記所定グループを特定するグループ名と前記機器固有 ID 部とを受信し、当該グループ名から取得されるグループ ID 部と前記機器固有 ID 部とを結合することにより行うことを特徴とする請求項 1 ～ 5 の何れかに記載のユーザ登録方法。

【請求項 7】 前記周辺機器が真正なグループ ID 部を保持しているかを確認した後、ユーザ登録を行うことを特徴とする請求項 6 に記載のユーザ登録方法。

【請求項 8】 前記周辺機器が真正なグループ ID 部を保持しているかを確認は、ランダムに発生させた所定コードを送信して当該所定コードとグループ ID 部とを用いた所定の方向計算をした結果を返信させることにより行うことを特徴とする請求項 7 に記載のユーザ登録方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、携帯電話やパソコン等の端末装置に接続された周辺機器に対して文書や画像を含むコンテンツを高セキュリティを維持したまま配信するコンテンツサーバへのユーザ登録方法に関し、特に、印刷出力機能を有する通信端末装置に印刷データを高セキュリティを確保して配信するコンテンツサーバへのユーザ登録方法に関する。

【0002】

【従来の技術】近年、携帯電話（PHS と呼ばれる簡易携帯電話も含む）が急速に普及し、かつ、その機能も本来の電話にとどまらず、インターネットアクセス機能等が付加され、携帯電話のみで、メール等のメッセージ送受信、各種ウェブ（Web）サイトへのアクセスが行えるようになった。特に、ウェブサイトへのアクセスは、携帯電話を利用した種々多様なサービスを受けることを可能とする。最近では、携帯電話向け専用のウェブサイトも数多く現れている。ウェブサイトの種類としては、例えば、銀行取引、証券取引、各種予約、娯楽関連情報提供、その他の種々多様なサービスを提供するものがある。

【0003】このようなウェブサイトの一つとして、現在、携帯電話の待ち受け画面に張り付けることができるキャラクタ等の画像を有料で配信するようなサービスも開始されている。また、一方で、携帯電話に接続して印刷出力を行える携帯電話用のプリンタも開発されている。

【0004】しかしながら、携帯電話に配信されているデータをそのまま印刷しても所望の印刷品質が確保できないという問題がある。また、印刷品質を管理した場合、いわゆる著作物の配信および課金体系が問題となり、携帯端末を介してデータを送信するプリンタに対するセキュリティの強化が重要となる。すなわち、従来、プリンタ出力機能を持たない携帯電話においてはキャラクタ画像を配信しても、それはその携帯電話での表示にのみ用いられるので、問題は少なかった。しかしながら、前述のように携帯電話からプリンタへ印刷出力が行えるようになると、一旦携帯電話に取り込んだキャラクタ等の画像は、反復して際限なく印刷出力できるようになる。これでは、有料サービスといっても従来と同様の課金体系では妥当ではなく、特定の印刷対象についての印刷出力に関して何らかの制限または管理が行えることが必要となる。また、不正プリンタを介しての不正アクセスを排除する必要がある。

【0005】また、パソコンなどの他の端末装置へコンテンツを配信する場合にも、不正複製を防止する暗号化データ配信が不可欠である。

【0006】

【発明が解決しようとする課題】しかしながら、このような暗号化データを配信する場合、暗号鍵をどのように決定するか、また、暗号鍵と関連付けてコンテンツサー

パへ安全にユーザ登録する方法が問題となる。

【0007】本発明は、このような事情に鑑み、携帯電話等の通信端末装置に対して接続される周辺機器に対して簡便な手法でセキュリティを強化した状態でコンテンツを配信できるコンテンツサーバへのユーザ登録方法を提供することを課題とする。

【0008】

【課題を解決するための手段】前記課題を解決する本発明の第1の態様は、ネットワークを介してコンテンツサーバへ接続する端末装置を介して、当該端末装置に接続され且つ暗号鍵となる機器ID及び復号化手段を具備する周辺機器の機器IDを前記コンテンツサーバへ登録するユーザ登録方法であって、前記周辺機器を接続した端末装置から前記ネットワークを介して接続して加入要求をしたユーザから、前記ユーザ識別IDと共に前記周辺機器の機器IDを取得する工程と、前記ユーザ識別ID及び前記機器IDの組合わせに対してユーザIDを決定する工程と、前記通信端末装置及び前記周辺機器の組合わせに対して前記ユーザIDを接続IDとすると共に前記機器IDをコンテンツ配信の暗号鍵としてユーザ登録する工程とを具備することを特徴とするユーザ登録方法にある。

【0009】本発明の第2の態様は、第1の態様において、前記端末装置がパソコンであり、USBポートに接続された暗号解読装置であることを特徴とするユーザ登録方法にある。

【0010】本発明の第3の態様は、第1の態様において、前記端末装置が通信端末装置であり、前記ユーザ識別IDを当該通信端末固有の端末IDとし、前記接続IDを、前記ユーザID及び前記端末IDを接続IDとすることを特徴とするユーザ登録方法にある。

【0011】本発明の第4の態様は、第1～3の何れかにおいて、前記ユーザIDを決定する際に接続するためのパスワードを決定することを特徴とするユーザ登録方法にある。

【0012】本発明の第5の態様は、第1～4の何れかの態様において、前記機器IDの取得は、前記周辺機器から機器IDを受信することにより行うことを特徴とするユーザ登録方法にある。

【0013】本発明の第6の態様は、第1～5の何れかの態様において、前記機器IDが所定グループに依存するグループID部と機器固有ID部とからなり、前記グループID部は前記所定グループ毎に予め登録されており、当該機器IDの取得は、前記周辺機器から前記所定グループを特定するグループ名と前記機器固有ID部とを受信し、当該グループ名から取得されるグループID部と前記機器固有ID部とを結合することにより行うことを特徴とするユーザ登録方法にある。

【0014】本発明の第7の態様は、第6の態様において、前記周辺機器が真正なグループID部を保持してい

るかを確認した後、ユーザ登録することを特徴とするユーザ登録方法にある。

【0015】本発明の第8の態様は、第7の態様において、前記周辺機器が真正なグループID部を保持しているかの確認は、ランダムに発生させた所定コードを送信して当該所定コードとグループID部とを用いた所定の一方計算をした結果を返信させることにより行うことを特徴とするユーザ登録方法にある。

【0016】かかる本発明によれば、コンテンツデータの配信に関してのセキュリティを簡便な手法で高度に保持して配信するコンテンツサーバへ、端末装置に接続される周辺機器からの高セキュリティを保持してユーザ登録することができる。

【0017】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照して詳細に説明する。この実施形態では、端末装置（以下、単に通信端末または端末ともいう）として、携帯電話を例として説明する。しかし、本発明はこれに限定されるものではなく、ゲーム機、テレビ、テレビのセットトップ端末、カーナビゲーション装置、等の種々の他の通信機能を有する端末、あるいはインターネットに接続する機能を備えたパソコン等にも適用することができる。また、周辺機器としては、プリンタを例示するが、プリンタに限定されず、各種記録媒体、音楽再生装置、画像再生装置など、通信端末装置に接続されて使用される全ての周辺機器に適用することができ、また、パソコンのUSBポートなどに接続されて暗号解読を行う暗号解読装置などに適用することができる。

【0018】まず、図1を参照して、本発明が適用されるコンテンツ配信システム全体の構成を説明する。本実施の形態における通信端末としての携帯電話10及び携帯電話10に接続された周辺機器であるプリンタ20は、専用ネットワーク101を介して各種のコンテンツサーバであるウェブサーバ100へ接続できる。専用ネットワーク101は、インターネットとは孤立したクローズド（閉鎖的）なネットワークを構成しており、オープンなインターネットからのアクセスはできないようになっている。すなわち、専用ネットワーク101には、特定の携帯電話からしかアクセスできないアクセスポイント102を介してのみ入ることができる。勿論、携帯電話10から図示しない中継サーバを経由して図示しないインターネットのWebサイトにもアクセスすることができるが、印刷出力管理に適する文書や画像等（コンテンツ）の印刷対象は、専用ネットワーク101側のウェブサーバ100上に置かれる。これにより、パソコンのような、コンテンツの自由な操作を制限できない機器から、当該印刷対象を保護することができる。

【0019】図2は、ウェブサーバ100と、携帯電話10及びプリンタ20の概略構成例を示す。

10

20

30

40

50

【0020】このウェブサーバ100は、高性能のデータ処理部110と、大容量のデータ格納部120とに大別され、データ処理部110には、携帯電話10に送信する各種情報のほか、各種コンテンツを構成する表示用画像データ111と、印刷用（高品位）画像データ112とが予め格納されている。

【0021】データ格納部120は、専用ネットワーク101（図1）に接続され、データの送受信を行う送受信部121と、データ格納部120に格納された各種情報及び表示用画像データ111を利用して携帯電話10へ送信する情報を処理する情報処理部122とを具備し、さらに、携帯電話10に接続されたプリンタ20との送受信を行うユーザ登録部123と、データ配信部124とを具備する。

【0022】ユーザ登録部123は、プリンタ20を接続した携帯電話10からのアクセス情報に基づいて新規ユーザか登録ユーザかを判断して、新規ユーザならユーザ登録を行い、登録ユーザならデータ配信部124にデータの配信を許可する。データ配信部124は、ユーザ登録部123の許可に基づいて印刷用画像データ112を所定の暗号化処理を施した後、配信する。

【0023】一方、携帯電話10は、ウェブサーバ100との送受信を行う送受信部11、接続されたプリンタ20を制御するプリンタ制御部12とを具備し、プリンタ20は、携帯電話10もしくは携帯電話10を介してウェブサーバ100との送受信を行う送受信部21と、受信した暗号化データを復号処理する復号処理部22と、復号処理された印刷用画像データを印刷する印刷処理部23とを具備し、さらに、プリンタ20は、固有のシリアルコードであるプリンタID25を内蔵する。

【0024】次に、携帯電話10とウェブサーバ100との間のデータの授受に関して説明する。携帯電話10とウェブサーバ100の間では、例えば、既知のHTTP (Hyper Text Transfer Protocol) プロトコルに則ってデータの授受が行われる。HTTPプロトコルにより送受されるデータは、主としてHTMLのようなマークアップ言語で記述された文書（ドキュメント）である。但し、本発明はHTML以外の他のマークアップ言語（例えば、XMLやSGML等）にも適用可能である。

【0025】携帯電話10は、自身に搭載された専用のウェブブラウザを用いてウェブサイト上のドキュメントにアクセスすることができ、さらに、このウェブブラウザに、後述するような印刷管理機能が組み込まれている。

【0026】携帯電話10のユーザは、所定の操作によって、特定のウェブサーバ100のアドレス（URL）またはサイトを指定すると、ウェブブラウザは、それにより特定されるウェブサーバ100の特定のページの内容（例えばHTMLファイル）の転送を要求する。これ

に対して、ウェブサーバ100は当該ページのHTMLファイルを携帯電話10へ返送する。ブラウザは、これを受けてその内容を解析し、携帯電話10の画面上に表示する。このページに、インライン画像が埋め込まれている場合には、その情報もウェブサーバ100に対して要求する。これに回答して、ウェブサーバ100はその表示用画像ファイルを返送する。ブラウザはこれを受けてページ内の指定された位置にその画像を表示する。ユーザが画面上に表示されたページ上にあるアンカーポイント（またはホットスポット）を指示したときには、さらに、そのリンク先である別のページやページ内箇所の情報を要求し、あるいは他のサイトへ飛ぶことができる。以上は、一般的なウェブ閲覧の動作である。

【0027】また、印刷時の携帯電話10とウェブサーバ100の動作を説明する。今、携帯電話10において、ウェブサーバ100から取り込まれた何らかのコンテンツを表示している状態を想定する。有料のウェブサイトでは、そのサイトへ入る際に有料である旨の警告がユーザに対してなされる。携帯電話10のユーザがその表示されているページや画像等の印刷対象の高品位画像を印刷する場合には、それを当該ウェブサーバ100に対して要求する。

【0028】ウェブサーバ100は、この要求を受信するとともに、プリンタ種別を確認し、このプリンタ種別に基づいて、これに合致した高品位画像データを作成または選択し、暗号処理して送信する。ここで、「作成」とは、基となる画像に対してプリンタ種別に合致するように解像度の変換や色数の変換等の加工を行うことであり、「選択」とは、予め複数のプリンタ種別用の画像データの中からプリンタ種別に合致したものを選ぶことである。

【0029】このとき、ユーザ登録部123は、プリンタ20を接続した携帯電話10からのアクセス情報に基づいて新規ユーザか登録ユーザかを判断して、新規ユーザならユーザ登録を行い、登録ユーザならデータ配信部124にデータの配信を許可する。データ配信部124は、ユーザ登録部123の許可に基づき、プリンタ種別を確認し、このプリンタ種別に基づいて、これに合致した高品位画像データを作成または選択し、暗号処理して送信する。ここで、「作成」とは、基となる画像に対してプリンタ種別に合致するように解像度の変換や色数の変換等の加工を行うことであり、「選択」とは、予め複数のプリンタ種別用の画像データの中からプリンタ種別に合致したものを選ぶことである。暗号化処理とは、プリンタIDを暗号鍵として印刷用画像データ112に所定の暗号化処理を施すことである。

【0030】このように暗号化処理された高品位画像データは携帯電話10に対して送信されるが、高品位画像データ自体は携帯電話10の表示画面には表示されず、プリンタ20の復号処理部22により復号処理され、印

刷が実行される。

【0031】このようなウェブサーバ100と、携帯電話10及びプリンタ20とのユーザ登録及び印刷要求の際の手順を図面を参照しながらさらに説明する。

【0032】図3は、本発明の一実施例に係るユーザ登録方法を示し、携帯電話10及びプリンタ20から新規にユーザ登録する流れを示す。なお、この例では、ウェブサーバ100をコンテンツサーバ100Aと認証サーバ100Bとで表示し、複数のコンテンツサーバ100Aに対する認証を一カ所の認証サーバ100Bで行うようにしたが、勿論、各コンテンツサーバ100Aが認証を行うようにしてもよい。

【0033】まず、プリンタ20を接続した携帯電話10からコンテンツサーバ100Aの所定のサイトにアクセスして加入要求を行う場合、プリンタ20にプリンタIDを要求し（ステップS1）、プリンタ20からプリンタIDを取得する（ステップS2）。この後、コンテンツサーバ100Aに対して加入要求とプリンタIDとを送信する（ステップS3）。このとき、コンテンツサーバ100Aでは携帯電話10固有の端末IDを自動的に取得しているため、この端末IDとプリンタIDとを認証サーバ100Bに送信してプリンタIDの登録を行う（ステップS4）。認証サーバ100Bでは、端末IDとプリンタIDとの組をユニークなIDとして登録する。このとき、携帯電話10とコンテンツサーバ100Aとの間のやり取りで決定され、再接続の際の同一性を判断するためのユーザ名及び必要に応じてパスワードを登録する。ユーザ名及びパスワードは、コンテンツサーバ100AがプリンタIDを取得した際に要求して決定するようにしてもよいし、プリンタIDを認証サーバ100Bに送信した後、認証サーバ100Bがコンテンツサーバ100Aを介して要求して決定するようにしてもよい。

【0034】図4には、登録ユーザが印刷データをダウンロードして印刷する手順を示す。

【0035】まず、プリンタ20を接続した携帯電話10からコンテンツサーバ100Aの所定のサイトにアクセスし、ユーザ名及びパスワードを送信すると共に印刷データの要求を行う（ステップS11）。このとき、プリンタIDの送信は行わない。コンテンツサーバ100Aは、ユーザID及びパスワード、さらに、自動的に取得している端末IDを認証サーバ100Bに送信し（ステップS12）、認証サーバ100Bは、認証を行って登録ユーザであることを確認したことを条件としてプリンタIDをコンテンツサーバ100Aに送信する（ステップS13）。次いで、コンテンツサーバ100Aでは受信したプリンタIDを暗号鍵として画像データを暗号処理し、暗号化したデータを携帯電話10に送信する（ステップS14）。携帯電話10を介して暗号化されたデータを受信したプリンタ20は、内蔵されるプリンタID

Dを暗号鍵として画像データを復号処理し、印刷する（ステップS15）。

【0036】以上、図3及び図4を参照して説明した方法では、極めて簡単な手法で高いセキュリティを確保することができる。すなわち、新規ユーザ登録時に一度だけ、プリンタIDが送信されるが、その後は、プリンタIDの送信を行うことなく、プリンタ20固有のプリンタIDを暗号鍵として暗号化された印刷データの送受信を行うので、印刷データが傍受されてもそのまま再利用することができない。なお、上述した認証サーバ100Bとコンテンツサーバ100Aとの間は専用線で接続されているので、プリンタIDの送信を行っても傍受等される虞は極めて小さい。

【0037】次に、プリンタIDそのものの送信を全く行うことなく、ユーザ登録を行ってさらにセキュリティを高めたユーザ登録方法の他の実施例を図5及び図6を参照しながら説明する。

【0038】この方法では、プリンタIDを一種のグループIDであるメーカーID部と、プリンタ固有ID部とで構成し、ユーザ登録の際にプリンタIDそのものを送信しないようにしたものである。すなわち、プリンタ20を接続した携帯電話10からコンテンツサーバ100Aの所定のサイトにアクセスして加入要求を行う場合、コンテンツサーバ100Aに対して加入要求と共にプリンタ固有ID部とメーカー名を送信する（ステップS31）。ここで、メーカー名とはメーカーIDではなく、メーカーを識別するためのテキストデータである。また、このとき必要に応じて、ユーザ名及びパスワードを予め決定しておく。コンテンツサーバ100Aではデータを受け付け、自動的に取得している携帯電話10固有の端末IDと、プリンタ固有ID及びメーカー名とを認証サーバ100Bに送信して認証要求を行う（ステップS32）。認証サーバ100Bでは、乱数からなるチャレンジコードを発生させ（ステップS33）、これを携帯電話10に送信する（ステップS34）。このとき、チャレンジコードの送信は携帯電話10に対して直接行っても、コンテンツサーバ100Aを介して送信してもよい。携帯電話10は受信したチャレンジコードをプリンタ20へ送信し（ステップS35）、プリンタ20では、受信したチャレンジコードと内蔵されるプリンタIDとを用いて、予め決められている所定の一方方向計算、例えば、ハッシュ関数により、所定のMD値を取得する（ステップS36）。このMD値は固有のメーカーIDから決定される値で、この値は、携帯電話10へ送信され（ステップS37）、携帯電話10から認証サーバ100Bへ送信される（ステップS38）。勿論、コンテンツサーバ100Aを介して送信するようにしてもよい。

【0039】一方、認証サーバ100Bは、各メーカーに与えられたメーカーIDを保有しており、最初に受信

したメーカー名から判断したメーカーIDと、先に携帯電話10へ送信したチャレンジコードからプリンタ20で実行されたものとの一方計算を行い(ステップS39)、同様にMD値を取得しておく(ステップS40)。そして、携帯電話10から受信したMD値と自ら取得したMD値とを照合して同一であることを条件として、ユーザー登録手続きを行い、先に取得したプリンタ固有ID部とメーカーID部とを合わせたプリンタIDをデータベースに登録する(ステップS42)。この際、先に取得した端末IDや、ユーザ名及びパスワードと関連付けて登録する点は上述した例と同様である。なお、ユーザ名及びパスワードは、MD値による認証を行った後、決定するようにしてもよい。

【0040】一方、MD値の照合で一致しなかった場合、プリンタ20が不正メーカーの製品という判断とし、ユーザー登録を拒否する(ステップS43)。

【0041】なお、ユーザー登録後の印刷データの取得は上述した例と同様である。

【0042】このように、この方法では、プリンタIDの一部を予め登録しておき、その部分を送信する必要がないので、プリンタIDそのものは一度も送信されることがなく、セキュリティがさらに高められたといえる。

【0043】また、この方法では、プリンタ20が実際に真正なメーカーであり、真正のメーカーIDを内蔵しているかの認証を行っているので、不正メーカー製品によるアクセスを拒否することができる。

【0044】しかしながら、真正のメーカーIDを内蔵しているかどうかの認証は必ずしも行う必要はない。すなわち、印刷データ自体は、メーカーIDを含むプリンタIDを暗号鍵として暗号化されて送信されるので、メーカーIDを内蔵しなければ印刷データを復号処理できないからである。従って、メーカーIDの認証ステップは省略してもよい。

【0045】以上説明した実施形態では、端末装置を携帯電話およびプリンタを例にとって説明したが、端末装置がパソコンであっても同様なユーザー登録方法およびコンテンツ配信を実施できる。すなわち、例えば、USBポートに接続する暗号解読装置に、機器IDおよび復号化プログラムを内蔵させ、暗号解読装置を接続したパソコンを介してコンテンツサーバに接続するようにする。ユーザー登録は、所望のユーザ名と機器IDとを用いるこ

とにより、上述した実施形態と同様に行うことができ、また、コンテンツ配信は、暗号解読装置に内蔵された機器IDを暗号鍵として暗号化したデータを配信することにより行う。これにより、ユーザ登録の際のセキュリティを高度に確保することができ、また、配信したコンテンツは配信を受けたときの暗号解読装置が接続されたパソコンでのみ利用できるのも、コンテンツの不正コピー等を防止することができる。

【0046】

【発明の効果】以上説明したように、本発明によれば、コンテンツデータの配信に関してのセキュリティを簡便な手法で高度に保持して配信するコンテンツサーバへ、端末装置に接続される周辺機器からの高セキュリティを保持してユーザ登録することができるという効果を奏する。

【図面の簡単な説明】

【図1】本発明のユーザー登録方法を採用するコンテンツ配信システム全体の構成を示すブロック図である。

【図2】携帯電話及びウェブサーバの構成例を示すブロック図である。

【図3】本発明の一実施形態に係るユーザー登録方法の手順を示す図である。

【図4】印刷データのダウンロードの手順を示す図である。

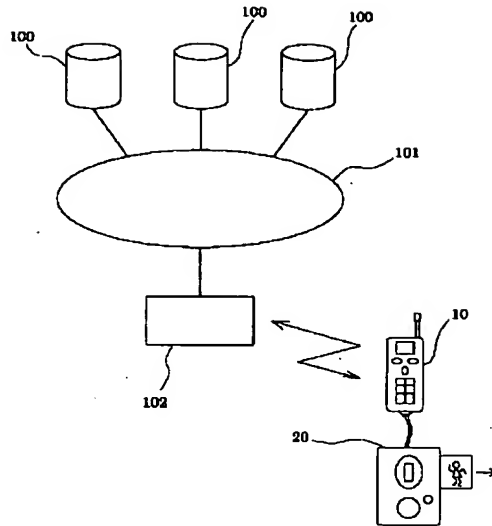
【図5】本発明の他の実施形態に係るユーザー登録方法の手順を示す図である。

【図6】本発明の他の実施形態に係るユーザー登録方法の手順を示す図である。

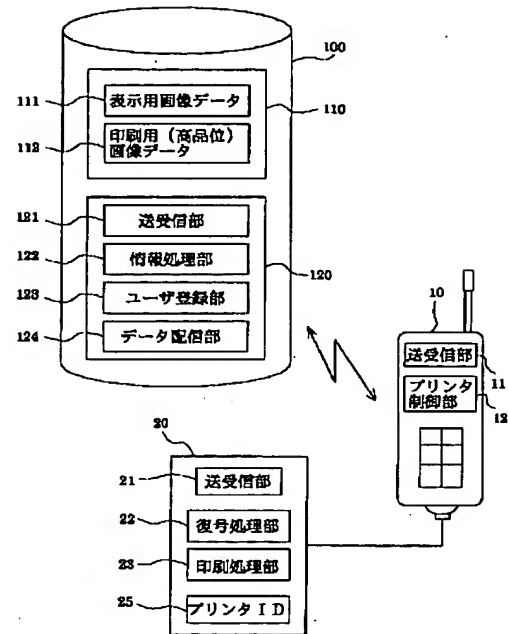
【符号の説明】

- 10 携帯電話
- 11 送受信部
- 12 プリンタ制御部
- 20 プリンタ
- 21 送受信部
- 22 復号処理部
- 23 印刷処理部
- 25 プリンタID
- 100 ウェブサーバ
- 100A コンテンツサーバ
- 100B 認証サーバ
- 101 専用ネットワーク
- 102 アクセスポイント

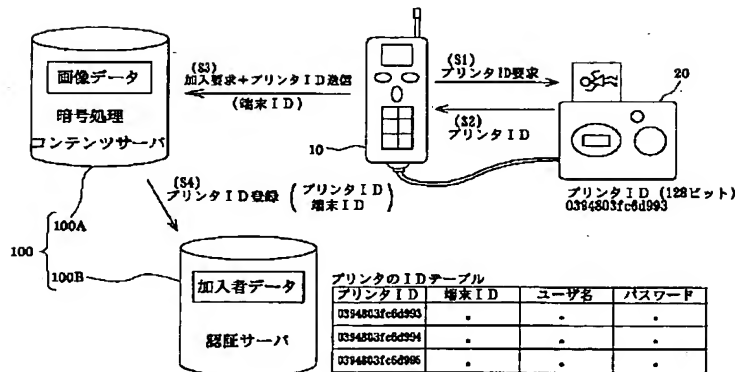
【図1】



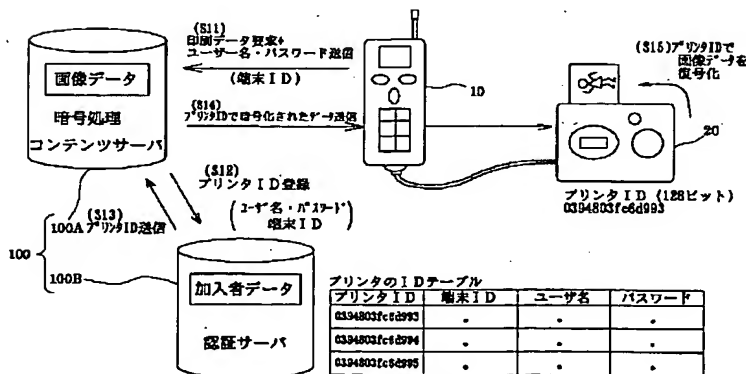
【図2】



【図3】



【図4】



[illegible]

```

graph TD
    S31[S31 加入要求] --> S32[S32 データ受付]
    S32 --> S33[S33 乱数]
    S33 --> S34[S34 チャレンジコード生成]
    S34 --> S35[S35 チャレンジコード送付]
    S35 --> S36[S36 MD値取得]
    S36 --> S37[S37 MD値送付]
    S37 --> S38[S38 MD値照会]
    S38 --> S39[S39 MD値照合]
    S39 -- No --> S41[S41 不正メーカー]
    S39 -- Yes --> S40[S40 ユーザ登録手続き開始]
    S40 --> S42[S42 DB登録]
  
```

Flowchart illustrating the process for issuing a portable telephone number:

- S31** 加入要求 (Request for joining)
- S32** データ受付 (Data reception)
- S33** 乱数 (Random number)
- S34** チャレンジコード生成 (Challenge code generation)
- S35** チャレンジコード送付 (Challenge code transmission)
- S36** MD値取得 (MD value acquisition)
- S37** MD値送付 (MD value transmission)
- S38** MD値照会 (MD value inquiry)
- S39** MD値照合 (MD value comparison)
- S40** ユーザ登録手続き開始 (Start of user registration procedure)
- S41** 不正メーカー (Unauthorized manufacturer)
- S42** DB登録 (DB registration)

F ターム(参考) 5J104 AA01 AA07 AA16 EA01 EA03
EA04 EA16 KA01 KA02 MA02
NA02 NA05 PA02 PA07
5K067 AA33 AA35 BB21 DD17 EE03
HH23 HH24